

INVARIABLE GENERATION WITH ELEMENTS OF COPRIME PRIME-POWER ORDER

ELOISA DETOMI AND ANDREA LUCCHINI

ABSTRACT. A finite group G is *coprimely-invariably generated* if there exists a set of generators $\{g_1, \dots, g_d\}$ of G with the property that the orders $|g_1|, \dots, |g_d|$ are pairwise coprime and that for all $x_1, \dots, x_d \in G$ the set $\{g_1^{x_1}, \dots, g_d^{x_d}\}$ generates G . In the particular case when $|g_1|, \dots, |g_d|$ can be chosen to be prime-powers we say that G is *prime-power coprimely-invariably generated*. We will discuss these properties, proving also that the second one is stronger than the first, but that in the particular case of finite soluble groups they are equivalent.

1. INTRODUCTION

Following [8] and [12], we say that a subset $\{g_1, \dots, g_d\}$ of a finite group G invariably generates G if $\{g_1^{x_1}, \dots, g_d^{x_d}\}$ generates G for every choice of $x_i \in G$. Then we say that a finite group G is *coprimely-invariably generated* (CIG, for short) if there exists a subset $X = \{g_1, \dots, g_d\}$ of G that invariably generates G and with the property that the orders $|g_1|, \dots, |g_d|$ are pairwise coprime; in the particular case when $|g_1|, \dots, |g_d|$ can be chosen to be prime-powers we say that G is “*prime-power*” *coprimely-invariably generated* (PCIG, for short). Using the classification of the finite simple groups, we will prove in Theorem 18 that all the finite non abelian simple groups are PCIG.

Clearly a PCIG group is in particular coprimely-invariably generated. In Proposition 6 we will prove the existence of a finite CIG group G which is not PCIG. However we obtain the unexpected result that a finite soluble CIG group is PCIG. Actually we prove a stronger result:

Theorem 1. *Let G be a finite soluble group and assume that there exists a set $\{g_1, \dots, g_d\}$ of invariable generators of G with the property that $|g_1|, \dots, |g_d|$ are pairwise coprime. For each $i \in \{1, \dots, d\}$, we write $g_i = x_{i,1} \cdots x_{i,u_i}$ where the $x_{i,j}$ are powers of g_i of coprime prime-power order. Then the set*

$$X = \{x_{i,j} \mid 1 \leq i \leq d, 1 \leq j \leq u_i\}$$

invariably generates G .

A key role in the proof of Theorem 1 is played by the theory of crowns, introduced by Gaschütz in [10]. Using the properties of the crowns, it can be proved (see Proposition 10) that a subset $\{g_1, \dots, g_d\}$ of a finite soluble group G invariably generates G if and only if $\{\phi(g_1), \dots, \phi(g_d)\}$ invariably generates $\phi(G)$ for any epimorphism $G \rightarrow V^t \rtimes H$, where H acts in the same way on each of the t direct factors and the action of H on V is faithful and irreducible. Thus, a crucial step is to

study, for a semidirect product $V^t \rtimes H$, under which conditions a coprime-invariable generating set of H can be lifted to a coprime-invariable generating set of $V^t \rtimes H$. Results in this direction are given in Proposition 8 and Proposition 9. Actually, Proposition 8 deals with the more general case of invariable generation, and might have some relevance in the study of invariable generation of soluble groups. For example, using this result, we can improve the bound given in [12, Theorem 3.1] for the smallest cardinality $d_I(G)$ of an invariably generating set of a finite group G : when G is soluble, the authors of [12] prove that $d_I(G) \leq a$, where a is the length of a chief series of G . Our stronger bound is:

Theorem 2. *If G is a finite soluble group then*

$$d_I(G) \leq \sum_{A \in \mathcal{V}} \left\lceil \frac{\delta_G(A)}{\dim_{\text{End}_G(A)} A} \right\rceil$$

where A runs in the set \mathcal{V} of representatives for the irreducible G -groups that are G -isomorphic to a complemented chief factor of G and, for $A \in \mathcal{V}$, $\delta_G(A)$ denote the number of complemented factors G -isomorphic to A in a chief series of G .

Using Proposition 9, as a byproduct we obtain a characterization of the finite supersoluble CIG groups.

Theorem 3. *Let G be a finite supersoluble group. Then G is coprimely-invariably generated if and only if no chief series of G contains two complemented and G -isomorphic chief factors.*

A motivation for our interest in PCIG groups is due to the fact a group without proper subgroups with the same exponent (we will call these groups *minimal-exponent groups*) is actually a PCIG group. Indeed assume that G is a minimal-exponent group with $e := \exp(G) = p_1^{n_1} \cdots p_t^{n_t}$. Then for every i , the group G contains an element g_i of order $p_i^{n_i}$. Clearly $\exp\langle g_1^{x_1}, \dots, g_t^{x_t} \rangle = e$, for every $x_1, \dots, x_t \in G$, so G is a PCIG group. On the other hand, there are PCIG groups which are not minimal-exponent. An easy example is given by the semidirect product G of two copies $C_3 \times C_3$ of a cyclic group of order 3 and a cyclic group $\langle y \rangle$ of order 2, acting trivially on the first component of $C_3 \times C_3$ and non-trivially on the second one. This group G can be invariably generated by y and a non-trivial diagonal element (x, x) in $C_3 \times C_3$. So G is PCIG, but has a proper (cyclic) subgroup, $\langle (x, 1)y \rangle$, with the same exponent.

In [7] the authors prove that if G is a CIG group, then the minimal size $d(G)$ of a generating set is at most 3, with $d(G) \leq 2$ whenever G is soluble. In particular, the same results hold for PCIG and minimal-exponent groups. As it is noticed in [7] the bound $d(G) \leq 3$ is sharp for both PCIG and CIG group. But it remains an open and difficult question to decide whether there exists a minimal-exponent group which is not 2-generated. We think that, in order to collect more information on this problem, it could be useful to investigate in more generality how far is the property of being minimal-exponent from the PCIG property. A substantial difference between the two properties is that only the second one is inherited by the epimorphic images, while an epimorphic image of a minimal-exponent group satisfies PCIG but is not in general minimal-exponent. Really we do not know examples of a PCIG group that does not appear as an epimorphic image of a minimal-exponent group and we propose the following question: is it true that for

every finite PCIG group X there exists a minimal-exponent finite group Y , and a normal subgroup N of Y , such that X is isomorphic to Y/N ?

The structure of the paper is the following. In Section 2 we investigate under which conditions a set of invariable generators of an epimorphic image can be lifted to the whole group; then we construct a CIG-group that is not PCIG and prove Theorem 1. Theorem 2 is proved in Section 3. In Section 4 we prove Theorem 3 and we analyse the structure of supersoluble minimal-exponent and CIG-groups. Finally, in Section 5 we prove that all the finite simple groups are PCIG and we present some further questions and examples.

2. CIG AND PCIG GROUPS

As noted above, a PCIG group is a CIG group. In this section we prove that there exists a CIG group which is not PCIG, but the two properties coincide on the class of soluble groups.

We start with some definitions and notations. In the following all groups are finite. A subset $X = \{g_1, \dots, g_d\}$ of G is an invariable generating set if $\{g_1^{x_1}, \dots, g_d^{x_d}\}$ generates G for every choice of $x_i \in G$. For brevity, we say that the subset $X = \{g_1, \dots, g_d\}$ is a CIG-set of G if X invariably generates G and the elements g_1, \dots, g_d have coprime orders; similarly, we say that a subset $X = \{g_1, \dots, g_d\}$ of G is a PCIG-set of G if X is a CIG-set of G and the orders $|g_1|, \dots, |g_d|$ are prime-powers.

Notation: Let H be a group acting irreducibly and faithfully on an elementary abelian p -group V . For a positive integer u we consider the semidirect product $G = V^u \rtimes H$: unless otherwise stated, we assume that the action of H is diagonal on V^u , that is, H acts in the same way on each of the u direct factors.

Lemma 4. *The group $G = V^u \rtimes H$ is coprimely-invariably generated if and only if there exist a CIG-set $\{h_1, \dots, h_d\} \in H$ and an element $v \in V^u$ such that*

- (1) $(|h_i|, p)$ if $i \neq 1$.
- (2) $\{h_1 v, h_2, \dots, h_d\}$ is a CIG-set for G .

Proof. Assume that $\{g_1, \dots, g_d\}$ is a CIG-set for $G = V^u \rtimes H$: thus $\{g_1, \dots, g_d\}$ invariably generates G and $|g_1|, \dots, |g_d|$ are coprime, in particular we can assume that $|g_i|$ is prime to p for every $i \neq 1$. For every i , we write $g_i = x_i v_i$ where $v_i \in V$ and $x_i \in H$. If $i \neq 1$, then g_i is conjugate to an element h_i of $\langle x_i \rangle$, since $\langle x_i \rangle$ is a Hall p' -subgroup of $V \langle x_i \rangle$ and g_i is a p' -element. As $\{g_1, \dots, g_d\}$ invariably generates G , the set $\{x_1 v_1, h_2, \dots, h_d\}$ is a CIG-set for G . Then, it is not difficult to see that $\{x_1, h_2, \dots, h_d\}$ must be a CIG-set for H . \square

Theorem 5. *Let $G = V^u \rtimes H$, where H acts irreducibly and faithfully on an elementary abelian p -group V and let $F = \text{End}_H(V)$. If G is coprimely-invariably generated, then*

$$u \leq \max_{h \in \Lambda} \dim_F C_V(h)$$

where Λ is the set of elements h in H contained in some CIG-set $\{h, h_2, \dots, h_d\}$ of H with $|h_i|$ prime to p for every $i \in \{2, \dots, d\}$.

Proof. If G is coprimely-invariably generated, then there exist h_1, \dots, h_d and v as in the statement of Lemma 4. Let $h = h_1$ and choose $w \in V$. Then $(hv)^w = h^w v =$

$h[h, w]v$, where $[h, w]v \in V$. Since

$$G = \langle (hv)^w, h_2, \dots, h_d \rangle \leq \langle [h, w]v, h, h_2, \dots, h_d \rangle \leq \langle [h, w]v \rangle^H H$$

we get that $\langle [h, w]v \rangle^H = V^u$, that is, $[h, w]v$ is a cyclic generator for the H -module V^u . Let $v = (v_1, \dots, v_u)$ and $w = (w_1, \dots, w_u)$. Switching to additive notation, the fact that $v + [h, w]$ is a generator for the H -module V^u implies that the elements $v_1 + [h, w_1], v_2 + [h, w_2], \dots, v_u + [h, w_u]$ are linearly independent in the F -vector space V . Let $\alpha_1, \dots, \alpha_u \in F$. Note that

$$\sum_{i=1}^u \alpha_i (v_i + [h, w_i]) = 0$$

if and only if

$$\sum_{i=1}^u \alpha_i v_i \in \left[h, \sum_{i=1}^u \alpha_i w_i \right].$$

Since this condition holds for every choice of $w \in V^u$, we deduce that v_1, \dots, v_u have to be linearly independent modulo the subspace $[h, V]$, hence

$$u \leq \dim_F V - \dim_F [h, V] = \dim_F C_V(h).$$

In particular $u \leq \max_{h \in \Lambda} \dim_F C_V(h)$, as required. \square

As an application of the previous result, we now prove that the properties CIG and PCIG are not equivalent.

Proposition 6. *There exists a coprimely-invariably generated group which is not PCIG.*

Proof. Note that $H = \text{Sym}(7)$ admits an absolute irreducible module V of order 7^5 (the full deleted permutation module). We use Theorem 5 to deduce that $G = V^5 \rtimes H$ is not PCIG. Indeed a set of elements of H of prime-power order that invariably generates H must contains an element x of order 7 (since all the other elements of H are contained in a point-stabilizer) and $\dim_{F_7} C_V(x) \leq 4$, since the action is faithful. Thus it follows from Theorem 5 that G is not PCIG.

However, if a_1, \dots, a_5 are F_7 -linearly independent elements of V , then $z = (a_1, \dots, a_5)$ generates V^5 as an H -module and $\{z, (1, 2, 3, 4, 5), (1, 2, 3)(4, 5, 6, 7)\}$ is a CIG-set of G . Thus G is a (non-soluble) CIG group. Note that in this case the trivial element e is contained in the CIG-set $\{e, (1, 2, 3, 4, 5), (1, 2, 3)(4, 5, 6, 7)\}$ of H , and $\dim_{F_7} C_V(e) = 5$, so that the condition of Theorem 5 is satisfied. \square

Theorem 5 gives a necessary condition on u in order to ensure that the semidirect product $G = V^u \rtimes H$ is a CIG group given that the irreducible linear group H is CIG. We are going to prove that this is indeed also a sufficient condition whenever $H^1(H, V) = 0$.

For the convenience of the reader, we provide the proof of the following key result:

Proposition 7. [5, Proposition 2.1]. *Suppose $H^1(H, V) = 0$ and $H = \langle h_1, \dots, h_d \rangle$. Let $w_i = (w_{i,1}, \dots, w_{i,u}) \in V^u$ with $1 \leq i \leq d$. The following are equivalent.*

- (1) $G \neq \langle h_1 w_1, \dots, h_d w_d \rangle$;
- (2) *there exist $\lambda_1, \dots, \lambda_u \in F = \text{End}_H(V)$ and $w \in V$ with $(\lambda_1, \dots, \lambda_u, w) \neq (0, \dots, 0, 0)$ such that $\sum_{1 \leq j \leq u} \lambda_j w_{i,j} = [h_i, w]$ for each $i \in \{1, \dots, d\}$.*

Proof. Let $K = \langle h_1 w_1, \dots, h_d w_d \rangle$. First we prove, by induction on u , that if $K \neq G$ then (2) holds. Let $z_i = h_i(w_{i,1}, \dots, w_{i,u-1}, 0)$ and let $Z = \langle z_1, \dots, z_d \rangle$. If $Z \not\cong V^{u-1}H$, then, by induction, there exist $\lambda_1, \dots, \lambda_{u-1} \in F$ and $w \in V$ with $(\lambda_1, \dots, \lambda_{u-1}, w) \neq (0, \dots, 0, 0)$ such that $\sum_{1 \leq j \leq u-1} \lambda_j w_{i,j} = [h_i, w]$ for each $i \in \{1, \dots, d\}$. In this case $\lambda_1, \dots, \lambda_{u-1}, 0$ and w are the requested elements.

So we may assume $Z \cong V^{u-1}H$. Set $V_u = \{(0, \dots, 0, v) \mid v \in V\}$. We have $ZV_u = KV_u = G$ and $Z \neq G$; this implies that Z is a complement of V_u in G and therefore there exists $\delta \in \text{Der}(Z, V_u)$ such that $\delta(z_i) = w_{i,u}$ for each $i \in \{1, \dots, d\}$. However, by Propositions 2.7 and 2.10 of [1], we have $H^1(Z, V_u) \cong F^{u-1}$. More precisely if $\delta \in \text{Der}(Z, V_u)$, then there exist an inner derivation $\delta_w \in \text{Der}(H, V)$ (for $w \in V$) and $\lambda_1, \dots, \lambda_{u-1} \in F$ such that for each $h(v_1, \dots, v_{u-1}, 0) \in Z$ we have

$$\delta(h(v_1, \dots, v_{u-1}, 0)) = \delta_w(h) + \lambda_1 v_1 + \dots + \lambda_{u-1} v_{u-1} = [h, w] + \lambda_1 v_1 + \dots + \lambda_{u-1} v_{u-1}.$$

In particular $-\sum_{1 \leq j \leq u-1} \lambda_j w_{i,j} + w_{i,u} = [h_i, w]$ for each $i \in \{1, \dots, d\}$, hence (2) holds.

Conversely, if (2) holds then $\langle h(v_1, \dots, v_u) \mid [h, w] = \lambda_1 v_1 + \dots + \lambda_u v_u \rangle$ is a proper subgroup of G containing K . \square

Let n be the dimension of V over $F = \text{End}_H(V)$. We have an injective homomorphism from H to $GL(n, F)$: we will use the notation \bar{h} to denote the image of $h \in H$ under this homomorphism. We will use the additive notation for $V = F^n$ and we will identify its elements with $1 \times n$ matrices with coefficient in F . With this notation, if $v \in V$ and $h \in H$, then v^h is the $1 \times n$ matrix $v\bar{h}$ obtained using the matrix multiplication; in particular, $[h, v] = v - v\bar{h} = v(1 - \bar{h})$.

Let $\pi_i : V^u \rightarrow V$ the canonical projection on the i -th component: $\pi_i(v_1, \dots, v_u) = v_i$.

If $w_i = (w_{i,1}, \dots, w_{i,u}) \in V^u$, $i = 1, \dots, d$, consider the vectors

$$r_j = (\pi_j(w_1), \dots, \pi_j(w_d)) = (w_{1,j}, \dots, w_{d,j}) \in V^d, j = 1, \dots, u.$$

Then Proposition 7 says that the elements $h_1 w_1, \dots, h_d w_d$ generate a proper subgroup of G if and only if there exists a non-zero vector $(\lambda_1, \dots, \lambda_u, w)$ in $F^u \times V$ such that

$$\sum_{1 \leq j \leq u} \lambda_j r_j = ([h_1, w], \dots, [h_d, w]).$$

This is equivalent to saying that there exist elements w_1, \dots, w_d in V^u such that $\langle h_1 w_1, \dots, h_d w_d \rangle = G$ if and only if there exist elements r_1, \dots, r_u in V^d that are linearly independent modulo the vector space

$$D = \{([h_1, w], \dots, [h_d, w]) \in V^d \mid w \in V\}.$$

Notice that $\dim_F(D) = \theta \dim_F(V)$ where $\theta = 0$ or 1 according to whether V is a trivial H -module or not: indeed, if H is non-trivial, then the linear map $\alpha : V \rightarrow V^d$, $w \mapsto ([h_1, w], \dots, [h_d, w])$ is injective (if $w \in \ker \alpha$ then $[h_i, w] = w$ for each $i \in \{1, \dots, d\}$, against the fact that h_1, \dots, h_d generate a non-trivial irreducible group). Therefore, there exist elements w_1, \dots, w_d in V^u such that $\langle h_1 w_1, \dots, h_d w_d \rangle = G$ if and only if $u \leq \dim_F(V^d) - \dim_F(D) = nd - \theta n$.

We now discuss the same question in the case of invariable generation: we are going to prove that $G = V^u \rtimes H$ admits a set of cardinality d invariably generating G if and only if, in the previous notations, there exists a set $\{h_1, \dots, h_d\}$

invariably generating H with the property that $u \leq nd - \sum_{1 \leq i \leq d} \dim_F [h_i, V] = \sum_i \dim_{\text{End}_H(V)} C_V(h_i)$.

Proposition 8. *Suppose that h_1, \dots, h_d invariably generate H and that $H^1(H, V) = 0$. Let $w_1, \dots, w_d \in V^u$ with $w_i = (w_{i,1}, \dots, w_{i,u})$. For $j \in \{1, \dots, u\}$, consider the vectors*

$$r_j = (\pi_j(w_1), \dots, \pi_j(w_d)) = (w_{1,j}, \dots, w_{d,j}) \in V^d.$$

Then $h_1 w_1, h_2 w_2, \dots, h_d w_d$ invariably generate $V^u \rtimes H$ if and only if the vectors r_1, \dots, r_u are linearly independent modulo

$$W = \{(u_1, \dots, u_d) \in V^d \mid u_i \in [h_i, V], i = 1, \dots, d\}.$$

In particular, there exist some elements $w_1, \dots, w_d \in V^u$ such that $h_1 w_1, h_2 w_2, \dots, h_d w_d$ invariably generate $V^u \rtimes H$ if and only if

$$u \leq nd - \dim W = \sum_i \dim_{\text{End}_H(V)} C_V(h_i).$$

Proof. Let $g_i = y_i x_i$ with $x_i \in H$ and $y_i = (y_{i,1}, \dots, y_{i,u}) \in V^u$ for $i \in \{1, \dots, d\}$ and let $X_{g_1, \dots, g_d} = \langle (h_1 w_1)^{g_1}, \dots, (h_d w_d)^{g_d} \rangle$. We have

$$(h_i w_i)^{g_i} = (h_i^{y_i} w_i)^{x_i} = h_i^{x_i} ([h_i, y_i] + w_i) \overline{x_i} = h_i^{x_i} z_i$$

where $z_i = ([h_i, y_i] + w_i) \overline{x_i} \in V^u$. Then $X_{g_1, \dots, g_d} = G$ if and only if the vectors of V^d

$$(\pi_j(z_1), \dots, \pi_j(z_d)) = ([h_1, y_{1,j}] + w_{1,j}) \overline{x_{1,j}}, \dots, ([h_d, y_{d,j}] + w_{d,j}) \overline{x_{d,j}},$$

$j = 1, \dots, u$, are linearly independent modulo the subspace

$$\begin{aligned} \tilde{D} &= \{([h_1^{x_1}, w], \dots, [h_d^{x_d}, w]) \in V^d \mid w \in V\} \\ &= \left\{ \left([h_1, w \overline{x_1^{-1}}] \overline{x_1}, \dots, [h_d, w \overline{x_d^{-1}}] \overline{x_d} \right) \in V^d \mid w \in V \right\}. \end{aligned}$$

Note that the map $f_{(x_1, \dots, x_d)} : V^d \mapsto V^d$ defined by

$$f_{(x_1, \dots, x_d)}(v_1, \dots, v_d) = (v_1 \overline{x_1}, \dots, v_d \overline{x_d})$$

is an isomorphism. Therefore the previous condition is equivalent to have that the vectors

$$([h_1, y_{1,j}] + w_{1,j}, \dots, [h_d, y_{d,j}] + w_{d,j}) = r_j + ([h_1, y_{1,j}], \dots, [h_d, y_{d,j}]),$$

for $j = 1, \dots, u$, are linearly independent modulo the subspace

$$D = \left\{ \left([h_1, w \overline{x_1^{-1}}], \dots, [h_d, w \overline{x_d^{-1}}] \right) \in V^d \mid w \in V \right\}.$$

Since this condition has to hold for every choice of $y_i \in V^u$ and $x_j \in H$, this means that the elements r_1, \dots, r_u have to be linearly independent modulo the subspace $W = \{(u_1, \dots, u_d) \in V^d \mid u_i \in [h_i, V], i = 1, \dots, d\}$, as required. \square

Example. Assume $H = \text{GL}(2, 2) \cong \text{Sym}(3)$ and let $V = F_2 \times F_2$. Suppose that (h_1, \dots, h_d) is a sequence of invariable generators of H where, let say, there are a entries of order 2, b entries of order 3 and c entries equal to the identity element, with $a + b + c = d$. Since h_1, \dots, h_d invariably generate H , then necessarily $a \geq 1$ and $b \geq 1$. According to the previous proposition, this sequence can be lifted to a sequence of invariable generators of $V^u \rtimes H$ if and only if $u \leq a + 2c$. Since $a + 2c = a + 2(d - a - b) = 2d - a - 2b$ has its maximal value at $a = b = 1$ and $c = d - 2$, $V^u \rtimes H$ can be invariably generated by d elements if and only if

$u \leq 1 + 2(d - 2) = 2d - 3$. In particular $G := V^2 \rtimes H$ cannot be invariably generated by 2 elements and consequently, since the prime divisors of $|G|$ are only 2 and 3, G has no coprime-invariable generating set, hence it is not CIG.

The previous proposition explains when and how a set of invariable generators for H can be lifted to a set of invariable generators for $V^u \rtimes H$. The situation changes if we consider the same question for coprime-invariable generating sets: in this case, by Lemma 4, when we try to lift a CIG-set $\{h_1, \dots, h_d\}$ of H to a CIG-set of $V^u \rtimes H$ we are free to modify via multiplication by elements of V^u only one of the d generators and consequently we get a more restrictive condition, as described by the following proposition.

Proposition 9. *Suppose that h_1, \dots, h_d have coprime order and invariably generate H and that $H^1(H, V) = 0$. Assume h_i is a p' -element for $i \neq 1$. Let $v = (v_1, \dots, v_u) \in V$. Then $h_1 v, h_2, \dots, h_d$ invariably generate $G = V^u \rtimes H$ if and only if the vectors v_1, \dots, v_u are linearly independent modulo $[h_1, V]$.*

Proof. It follows from the proof of Theorem 5 that the condition that the vectors v_1, \dots, v_u are linearly independent modulo $[h_1, V]$ is necessary to have that $h_1 v, h_2, \dots, h_d$ invariably generate G . On the other hand, in the notation of Proposition 8, if the vectors v_1, \dots, v_u are linearly independent modulo $[h_1, V]$, then $v_1^* = (v_1, 0, \dots, 0), \dots, v_u^* = (v_u, 0, \dots, 0)$ are linearly independent modulo W , hence $h_1 v, h_2, \dots, h_d$ is a CIG-set of G . \square

Now we apply the theory of crowns to reduce the problem of invariable generation for a soluble groups G to the particular case of a semidirect product $V^u \rtimes H$, as studied above.

Let G be a finite soluble group, and let \mathcal{V} be a set of representatives for the irreducible G -groups that are G -isomorphic to a complemented chief factor of G . For $V \in \mathcal{V}$ let $R_G(V)$ be the smallest normal subgroup contained in $C_G(V)$ with the property that $C_G(V)/R_G(V)$ is G -isomorphic to a direct product of copies of V and it has a complement H in $G/R_G(V)$. The factor group $C_G(V)/R_G(V)$ is usually called “crown” of G associated to the G -module V (for more details, see [2]). The non-negative integer $\delta_G(V)$ defined by $C_G(V)/R_G(V) \cong_G V^{\delta_G(V)}$ is called the V -rank of G and it coincides with the number of complemented factors in any chief series of G that are G -isomorphic to V . Actually, $G/R_G(V) \cong V^{\delta_G(V)} \rtimes H$, where H acts diagonally on each component of $V^{\delta_G(V)}$ (see [10]).

Proposition 10. [14, Proposition 2.4] *Let G and \mathcal{V} be as above. Let x_1, \dots, x_d be elements of G such that $\langle x_1, \dots, x_d, R_G(V) \rangle = G$ for any $V \in \mathcal{V}$. Then $\langle x_1, \dots, x_d \rangle = G$.*

The previous result allows us to reduce the proof of Theorem 1 to the quotient groups $G/R_G(V)$.

Proof of Theorem 1. Let G be a soluble group. We want to prove that if $\{g_1, \dots, g_d\}$ is a CIG-set of G , then the set $X = \{x_{ij} \mid 1 \leq i \leq d, 1 \leq j \leq u_i\}$ is a PCIG-set of G , where the x_{ij} , $1 \leq j \leq u_i$, are the powers of g_i of prime power order.

The proof is by induction on $|G|$, case $|G| = 1$ being trivial. By Proposition 10 it is not restrictive to assume that $G = V^u \rtimes H$ where H is an irreducible subgroup of $\text{GL}(V)$ and V is a p -group. Note that, as G is soluble, $H^1(H, V) = 0$ [16, Lemma 1]. We may assume that p does not divide $|g_i|$ if $i \neq 1$: in particular it is not

restrictive to assume $g_i \in H$ if $i \neq 1$. Moreover it is not restrictive to assume that $g_1 = abv$ with $a, b \in H$, $v \in V$, a and bv elements of $\langle g_1 \rangle$, $(|a|, p) = 1$, and $|bv|$ a p -power.

Let $v = (v_1, \dots, v_u)$. As ab, g_2, \dots, g_d invariably generate H , by Lemma 9, the vectors v_1, \dots, v_u are linearly independent modulo $[ab, V]$. We may assume $x_{1,1} = bv$ and $x_{i,j} \in H$, $(|x_{i,j}|, p)$ if $(i, j) \neq (1, 1)$.

By induction

$$\{b, x_{i,j} \mid 1 \leq i \leq d, 1 \leq j \leq u_i, (i, j) \neq (1, 1)\}$$

is PCIG-set of H . Since $bv \in \langle abv \rangle$, there exists $n \in \mathbb{N}$ such that $b = (ab)^n$. We may identify ab and b with two matrices X and Y such that $Y = X^n$. In this identification $[ab, V]$ correspond to the image $V(1 - X)$ of the linear map $1 - X$ and $[b, V]$ to the image $V(1 - Y)$ of the linear map $1 - Y$. Clearly we have

$$V(1 - Y) = V(1 - X^n) = V(1 + X + \dots + X^{n-1})(1 - X) \leq V(1 - X),$$

i.e. $[b, V] \leq [ab, V]$, hence the vectors v_1, \dots, v_u , being linearly independent modulo $[ab, V]$, are linearly independent modulo $[b, V]$ too. By Lemma 9 we conclude that the set

$$\{bv, x_{i,j} \mid 1 \leq i \leq d, 1 \leq j \leq u_i, (i, j) \neq (1, 1)\} = \{x_{i,j} \mid 1 \leq i \leq d, 1 \leq j \leq u_i\}$$

invariably generates G , and is actually a PCIG-set of G , as required. \square

3. A BOUND FOR $d_I(G)$ WHEN G IS A SOLUBLE GROUP

In this section we will prove Theorem 2 that bounds the smallest cardinality $d_I(G)$ of an invariably generating set of a finite soluble group G by a function of the numbers $\delta_G(A)$ of complemented factors G -isomorphic to A in a chief series of G , where A runs in the set \mathcal{V} of representatives for the irreducible G -groups that are G -isomorphic to a complemented chief factor of G .

First we need to recall the following results:

Lemma 11. [2, Lemma 1.3.6] *Let G be a finite soluble group with trivial Frattini subgroup. There exists a crown C/R and a non trivial normal subgroup U of G such that $C = R \times U$.*

Lemma 12. [6, Proposition 11] *Assume that G is a finite soluble group with trivial Frattini subgroup and let C, R, U be as in the statement of Lemma 11. If $KU = KR = G$, then $K = G$.*

Proof of Theorem 2. The proof is by induction on $|G|$. Let

$$\eta = \eta(G) = \sum_{A \in \mathcal{V}} \left\lceil \frac{\delta_G(A)}{\dim_{\text{End}_G(A)} A} \right\rceil.$$

If $\text{Frat}(G) \neq 1$, then by induction $d_I(G/\text{Frat}(G)) \leq \eta(G/\text{Frat}(G))$. As

$$\eta(G/\text{Frat}(G)) = \eta(G) \text{ and } d_I(G/\text{Frat}(G)) = d_I(G),$$

we immediately conclude $d_I(G) \leq \eta$.

Assume now $\text{Frat}(G) = 1$. In this case, by Lemma 11, there exists a crown C/R of G and a normal subgroup U of G such that $C = R \times U$. We have $R = R_G(V)$, $C = C_G(V)$ where $V \in \mathcal{V}$ is an irreducible G -module and $U \cong_G V^\delta$ for $\delta = \delta_G(V)$. Moreover $G/R \cong U \rtimes H$ where H acts in the same way on each of the δ factors of

U and this action is faithful and irreducible. Let $r = \dim_{\text{End}_G(V)} V$ and $\alpha = \lceil \delta/r \rceil$. Set $\beta = \eta(G/U)$ and note that

$$\eta = \beta + \alpha.$$

By induction, $d_I(G/U) \leq \eta(G/U) = \beta$. In particular G contains β elements x_1, \dots, x_β that invariably generate G modulo U . Now set $x_{\beta+1} = \dots = x_\eta = 1$: of course the $\eta = \beta + \alpha$ elements $x_1, \dots, x_\beta, x_{\beta+1}, \dots, x_\eta$ are still invariable generators of G . Clearly for every $i = \beta + 1, \dots, \eta$, we have that $\dim_{\text{End}_G(V)} C_V(x_i) = \dim_{\text{End}_G(V)} V = r$, hence

$$\sum_{1 \leq i \leq \eta} \dim_{\text{End}_G(V)} C_V(x_i) \geq \sum_{\beta+1 \leq i \leq \eta} \dim_{\text{End}_G(V)} C_V(x_i) \geq \alpha \cdot r \geq \delta$$

and therefore, by Proposition 8, there exist $u_1, \dots, u_\eta \in U$ such that $x_1 u_1, \dots, x_\eta u_\eta$ invariably generate G modulo R . Let $g_1, \dots, g_\eta \in G$ and consider the subgroup $K = \langle (x_1 u_1)^{g_1}, \dots, (x_\eta u_\eta)^{g_\eta} \rangle$. By construction, x_1, \dots, x_η invariably generate G modulo U , hence $KU = \langle x_1^{g_1}, \dots, x_\eta^{g_\eta} \rangle U = G$. Since $x_1 u_1, \dots, x_\eta u_\eta$ invariably generate G modulo R , we have also $KR = G$. We conclude from Lemma 12 that $G = K$. Hence $x_1 u_1, \dots, x_\eta u_\eta$ invariably generate G . \square

4. SUPERSOLUBLE GROUPS

We start this section with an easy observation.

Proposition 13. *A nilpotent group G is coprimely-invariably generated if and only if it is cyclic.*

Proof. Clearly an abelian group is CIG if and only if it is cyclic. If G is a nilpotent CIG group, then $G/\text{Frat}(G)$ is abelian and CIG, hence $G/\text{Frat}(G)$, and consequently G , is cyclic. \square

What happens if we replace nilpotency with supersolubility? How “thin” is a supersoluble CIG group? A first answer is given by Theorem 3, where it is proved that $\delta_G(V) = 1$ for every complemented chief factor V of G .

Proof of Theorem 3. Let G be a finite supersoluble CIG group and assume by contradiction that a chief series of G contains two different complemented chief factors isomorphic to an irreducible G -module V . Let $H = G/C_G(V)$. The semidirect product $V^2 \rtimes H$ is an epimorphic image of G , hence it is CIG. It follows from Theorem 5 that $2 \leq \dim_{\text{End}_H(V)} V$, however since G is supersoluble, V is cyclic and $\dim_{\text{End}_H(V)} V = 1$, a contradiction.

Conversely, assume that no chief series of G contains two complemented and G -isomorphic chief factors. Let p be the largest prime divisor of G : the Sylow p -subgroup P of G is normal. By induction, a p -complement H of P in G has a CIG-set, say $\{h_1, \dots, h_d\}$. Moreover there exists x in G such that $\langle x \rangle^H = P$. Indeed $P/\text{Frat}(P) \cong V_1 \times \dots \times V_u$ where $|V_i| = p$ for each $i \in \{1, \dots, u\}$ and, by our hypothesis, V_i and V_j are not H -isomorphic if $i \neq j$: this implies that $P/\text{Frat}(P)$ is a cyclic H -module. It can be easily verified that $\{x, h_1, \dots, h_d\}$ is a CIG-set of G . \square

As a corollary, we have a bound on the minimal number of generators of the Sylow p -subgroups.

Corollary 14. *Let G be a supersoluble and coprimely-invariably generated finite group. Then for any prime p dividing $|G|$, a Sylow p -subgroup of G can be generated by $p - 1$ elements.*

Proof. If $p_1 < p_2 < \dots < p_t$ are the prime divisors of $|G|$, then there exists a normal series $1 = N_t < \dots < N_0 = G$ with the property that N_{i-1}/N_i is a Sylow p_i -subgroup of G/N_i . Let $P_i = N_{i-1}/N_i$ and let $V_i = P_i/\text{Frat } P_i$. Since G is supersoluble, $V_i = U_{i,1} \times \dots \times U_{i,t_i}$, with $|U_{i,j}| = p_j$ for each $j \in \{1, \dots, t_i\}$; moreover, by Proposition 3, U_{i,j_1} and U_{i,j_2} are not G -isomorphic if $j_1 \neq j_2$. In particular $G/C_G(V_i)$ is abelian, and consequently cyclic by Proposition 13. However a cyclic group has at most $p_i - 1$ 1-dimensional inequivalent representations over the field with p_i -elements, so $d(P_i) = d(V_i) = t_i \leq p_i - 1$. \square

In the remaining part of this section we will prove that the previous result is best possible: for any prime p it can be constructed a supersoluble coprimely-invariably generated finite G with the property that $d(P) = p - 1$ for every Sylow p -subgroup P of G . Notice that this group is actually minimal-exponent.

In order to construct these examples we need to recall some properties of the Sylow p -subgroup P_m of $\text{Sym}(p^m)$ and its normalizer N_m in $\text{Sym}(p^m)$. We have that P_m is isomorphic to the iterated wreath product $C_p \wr \dots \wr C_p$ of m copies of the cyclic group of order p . In particular $P_m \cong B_m \rtimes P_{m-1}$ with $B_m \cong (\mathbb{Z}/p\mathbb{Z})^{p^{m-1}}$. Notice that

$$I_m = \left\{ (x_1, \dots, x_{p^{m-1}}) \in B_m \mid \sum_i x_i = 0 \right\}$$

is the unique maximal P_{m-1} -submodule of B_m . Let $y_m = (1, 0, \dots, 0) \in B_m$. Clearly $B_m = I_m \times \langle y_m \rangle$. Moreover $F_m = I_m I_{m-1} \dots I_1$ is the Frattini subgroup of P_m and $\gamma_1, \dots, \gamma_m$ is a basis for $P_m/F_m \cong C_p^m$, where $\gamma_i = y_i F_m$. Let N_m be the normalizer of P_m in $\text{Sym}(p^m)$. We have that N_m is a split extension of P_m with a direct product H_m of m copies of the cyclic group of order $p - 1$ (see for example [4]). From the description of the action of H_m over P_m given in [3] before the statement of Proposition 2.4 it follows that for every $(\beta_1, \dots, \beta_m) \in (\mathbb{Z}/p\mathbb{Z})^*$, there exists $h \in H$ such that $\gamma_i^h = \beta_i \gamma_i$ for every $1 \leq i \leq m$. In particular $B_m^h = B_m$, so h induces an automorphism \bar{h} of $P_m/B_m \cong P_{m-1}$.

Lemma 15. *Let $m \leq p - 1$ and let $h \in H_m$ such that $\gamma_1^h = \beta_1 \gamma_1, \dots, \gamma_m^h = \beta_m \gamma_m$ with $\beta_i \neq \beta_j$ whenever $i \neq j$. Then the group $G = P_m \rtimes \langle h \rangle$ is minimal-exponent.*

Proof. Let $\alpha = |h|$. Since $\exp(P_m) = p^m$, we have that $\exp(G) = p^m \alpha$. Let $H \leq G$ with $\exp(H) = \exp(G)$. In particular H must contain an element of order α : the subgroups of G with order α are conjugate, so it is not restrictive to assume $h \in H$. Let $Q = P_m \cap H$ and consider $B = B_m \cap Q$. Since Q contains an element of order p^m , the factor group Q/B must contain an element of order p^{m-1} . Let \bar{h} be the automorphism group of P_m/B_m induces by h . We have that $\overline{H} = QB_m/B_m \rtimes \langle \bar{h} \rangle$ is a subgroup of $\overline{G} = P_m/B_m \rtimes \langle \bar{h} \rangle$ with $\exp(\overline{H}) = \exp(\overline{G})$. By induction $\overline{H} = \overline{G}$, hence $QB_m = P_m$. Let now x be a p^m -cycle contained in Q . We can write $x = by$ with $b = (u_1, \dots, u_{p^{m-1}}) \in B_m$ and y a p^{m-1} -cycle in P_{m-1} . Since $|x| = p^m$ we must have $(by)^{p^{m-1}} \neq (0, \dots, 0)$ and this implies $\sum_i u_i \neq 0$ i.e. $b \notin I_m$. This means that $xF_m = x_1 \gamma_1 + \dots + x_m \gamma_m$ with $x_1 \neq 0$. Applying the subsequent Lemma

17 to the $\langle h \rangle$ -invariant subspace $W = QF_m/F_m$ of $V = P_m/F_m$, we deduce that $\gamma_m \in QF_m/F_m$: hence $P_m = QB_m = QF_m = Q$ and $H = G$. \square

Corollary 16. *Let p be an odd prime. The p -group P_{p-1} admits an automorphism h of order $p-1$ with the property that $G = P_{p-1} \rtimes \langle h \rangle$ is a minimal-exponent group. This group G is supersoluble with exponent $(p-1)p^{p-1}$ and order $(p-1)p^{\frac{p^p-1}{p-1}}$.*

Lemma 17. *Let $V = F^n$ be an n -dimensional vector space over the field F and let $\alpha = \text{diag}(\beta_1, \dots, \beta_n)$. Suppose that $\beta_i \neq 0$ for each $i \in \{1, \dots, n\}$ and that $\beta_i \neq \beta_j$ whenever $i \neq j$. Suppose that an α -invariant subspace W of V contains an element $v = (x_1, \dots, x_n)$ with $x_1 \neq 0$. Then $(1, 0, \dots, 0) \in W$.*

Proof. Let $\Omega := \{(y_1, \dots, y_m) \in W \mid y_1 \neq 0\}$ and assume that $\omega = (z_1, \dots, z_n)$ is an element of Ω with the property that the cardinality of the set $J_\omega = \{i \neq 1 \mid z_i \neq 0\}$ is as smallest as possible. Assume by contradiction that $J_\omega \neq \emptyset$ and choose $i \in J_\omega$. We have

$$\bar{\omega} = \beta_i \omega - \omega^\alpha = (\beta_i z_1, \dots, \beta_i z_n) - (\beta_1 z_1, \dots, \beta_n z_n) \in W.$$

Since $\beta_i - \beta_1 \neq 0$, we have $\bar{\omega} \in \Omega$. Moreover $J_{\bar{\omega}} \subseteq J_\omega$ but $i \in J_\omega \setminus J_{\bar{\omega}}$, against the minimality of $|J_\omega|$. \square

5. FURTHER EXAMPLES AND SOME QUESTIONS

In this section we prove that all the finite simple groups are PCIG and we make some further considerations on the differences among the properties PCIG and CIG and the property of being minimal-exponent.

In [12] the authors prove that every non-abelian finite simple group G is invariably generated by 2 elements; for many simple groups, the two generators exhibited in [12] have coprime orders. Examining the remaining cases, in [7] it is proved that a finite nonabelian simple groups G contains four elements of pairwise coprime order invariably generating G (in fact three element suffices if $G \neq \text{P}\Omega_8^+(2), \text{P}\Omega_8^+(3)$).

Theorem 18. *All the finite simple groups satisfies PCIG.*

Proof. Let G be a finite simple groups. Clearly if G is cyclic of order p , then G is PCIG, so we may assume that G is non abelian. First consider the case $G = \text{Alt}(n)$. If $n \geq 7$, then there exists a prime p with $n/2 < p < n-2$ (e.g. by Nagura's result [15]). Write $n = p_1^{n_1} \dots p_r^{n_r}$ as a product of powers of different primes and consider the following elements: y, x_1, \dots, x_r where y has order p , x_i is the product of $n/p_i^{n_i}$ disjoint cycles of length $p_i^{n_i}$ if p_i is odd, x_i is the product of $n/2^{n_i-1}$ disjoint cycles of length 2^{n_i-1} if $p_i = 2$. Let now $a, b_1, \dots, b_r \in \text{Alt}(n)$ and consider $H = \langle y^a, x_1^{b_1}, \dots, x_r^{b_r} \rangle$ and let Δ be an H -orbit: we have that $|x_i|$ divides $|\Delta|$ for each $i \in \{1, \dots, r\}$ and $|\Delta| \geq p > n/2$, hence $|\Delta| = n$. This implies that G is transitive (and consequently primitive since it contains a p -cycle): but then $H = \text{Alt}(n)$ by [9, Theorem 3.3E], hence y, x_1, \dots, x_r invariably generate $\text{Alt}(n)$. If $n \in \{5, 6\}$ then $\text{Alt}(n)$ is invariably generated by any subset $\{x_1, x_2, x_3\}$ with x_1 of order 5, x_2 of order 3 and x_3 of order 2 if $n = 5$, of order 4 if $n = 6$. To deal with the other simple groups we use [13, Corollary 5]: all the pairs (G, M) where G is a finite non abelian simple group and M is a proper subgroup of G with $\pi(G) = \pi(M)$ are listed in [13, Table 10.7]. Now, for a given simple group G , consider a set $\Omega_G = \{x_p \mid p \in \pi(G)\}$, where x_p is a nontrivial p -element of G . If G does not appear in [13, Table 10.7], then Ω_G is a PCIG-set of G , independently

of our choice of the elements x_p . Let \mathcal{S} be the set of simple groups that are not alternating groups and contain a proper subgroup M with $\pi(G) = \pi(M)$. By [13, Table 10.7] if $G \in \mathcal{S} \setminus \{\mathrm{P}\Omega_8^+(2), \mathrm{PSL}_6(2), \mathrm{PSp}_6(2), \mathrm{M}_{12}\}$, then, up to conjugacy in $\mathrm{Aut}(G)$, there exists a unique proper subgroup M of G with $\pi(G) = \pi(M)$; moreover by [11, Theorem 1.3], except when $G = \mathrm{P}\Omega_8^+(3)$, there exist a prime p and a p -element $g \in G$ such that $g \notin \cup_{\phi \in \mathrm{Aut}(G)} M^\phi$ (indeed g can be chosen of order p is $G \neq \mathrm{M}_{11}$, of order 8 otherwise). If $x_p = g$, then Ω_G is a PCIG-set for G . If $G \in \{\mathrm{PSL}_6(2), \mathrm{PSp}_6(2)\}$, then G contains an element G of order 9 while no proper subgroup M of G with $\pi(G) = \pi(M)$ contains element of order 9: if we choose x_3 of order 9, then Ω_G is a PCIG-set. The group $G = \mathrm{M}_{12}$ contains, up to conjugacy in $\mathrm{Aut}(G)$, two subgroups M with $\pi(G) = \pi(M)$: $M_1 \cong \mathrm{PSL}(2, 11)$ and $M_2 \cong \mathrm{M}_{11}$; on the other hand G contains g_1 of order 2 and g_2 of order 3 with the property that $g_i \notin \cup_{\phi \in \mathrm{Aut}(G)} M_i^\phi$ for $i = 1, 2$. If we choose $x_2 = g_1$ and $x_3 = g_2$, then Ω_G is a PCIG-set. The cases $G = \mathrm{P}\Omega_8^+(2), \mathrm{P}\Omega_8^+(3)$ are discussed in [7]: they are invariably generated by four elements of orders, respectively, 2, 5, 7, 9 and 5, 7, 9, 13. \square

As remarked in the introduction, if G is a minimal-exponent group, then G is PCIG, but the converse does not hold. Moreover, it is easy to see that epimorphic images of PCIG groups (or CIG groups) are PCIG (CIG, respectively). Actually, the converse holds when we consider quotients over Frattini subgroups.

Lemma 19. *A finite group G is PCIG (CIG) if and only if $G/\mathrm{Frat}(G)$ is PCIG (CIG).*

Proof. Let $F = \mathrm{Frat}(G)$. Assume that $\{g_1F, \dots, g_dF\}$ is a PCIG-set of G/F and let $|g_iF| = p_i^{n_i}$. For every $i = 1, \dots, d$, we can write $g_i = x_i y_i$ with $|x_i|$ a p_i -power and $|y_i|$ coprime with p_i ; in particular $y_i \in F$. It can be easily proved that x_1, \dots, x_d is a PCIG-set of G . The other implication is trivial. Similar arguments hold for CIG groups. \square

On the other hand, the property of being minimal-exponent is not closed under epimorphic images, even when the kernel is contained in the Frattini subgroup: indeed, there exists a minimal-exponent group G such that $G/\mathrm{Frat}(G)$ is not minimal-exponent. For example, let G be the supersoluble minimal-exponent group constructed in Corollary 16 for $p = 3$: then G has order $3^4 \cdot 2$ and exponent 18. However, if P is the Sylow 3-subgroup of G , then $\mathrm{Frat}(G) = \mathrm{Frat}(P)$ and $G/\mathrm{Frat}(G)$ is a group of order 18 and exponent 6 containing an element of order 6: in particular $G/\mathrm{Frat}(G)$ is not minimal-exponent. Even the converse implication is false: there exists a finite group G which is not minimal-exponent but $G/\mathrm{Frat}(G)$ is minimal-exponent. For example, consider the dihedral group K of order 12. Since $K/Z(K) \cong \mathrm{GL}(2, 2)$ we have an action of K on $H = C_2 \times C_2$ with kernel $Z(K)$. Let G be the semidirect product $H \rtimes K$. Since $\exp(G) = \exp(K) = 12$, G is not minimal-exponent. However $\mathrm{Frat}(G) = Z(K)$, hence $G/\mathrm{Frat}(G) \cong \mathrm{Sym}(4)$ is a minimal-exponent group.

Notice that every epimorphic image of a minimal-exponent group is PCIG. We have seen that examples of PCIG groups that are not minimal-exponent can be easily constructed. However we don't know the answer to the following intriguing question:

Question 1. *Is it true that any PCIG group appears as an epimorphic image of a minimal-exponent group?*

In the following we want to discuss some examples and analyze some particular instances of the previous question.

The first case that one would like to solve is that of finite simple groups. By Theorem 18 every finite simple group satisfies PCIG, however a finite non abelian simple groups is not necessarily minimal-exponent (for example $\exp(\text{Alt}(n-1)) = \exp(\text{Alt}(n))$ except when $n = p^t$ with p an odd prime or $n = 2^t + 2$ and $n-1$ is a prime-power). It should be interesting to answer to the following questions.

Question 2. *Is it true that for any simple group S there exists a minimal-exponent finite group G admitting S as a composition factor?*

Question 3. *Is it true that for any simple group S there exists a minimal-exponent finite group G admitting S as an epimorphic image?*

Consider for example $G := \text{Alt}(8)$; G is not minimal-exponent, since $\exp(\text{Alt}(8)) = \exp(\text{Alt}(7)) = 420$, however G is a composition factor of $\text{Sym}(8)$, which is a minimal exponent group. On the other hand, we don't know examples of minimal-exponent groups admitting $\text{Alt}(8)$ as epimorphic image. Similarly, $\exp(M_{11}) = \exp(M_{12})$ and $\exp(M_{23}) = \exp(M_{24})$ and we don't know examples of minimal-exponent groups admitting M_{12} or M_{24} as composition factor.

More in general, given a simple group S , we may define $\beta_G(S)$ as the number of normal subgroups N of G with $G/N \cong S$. If G is a CIG group and S is abelian, then $\beta_G(S) \leq 1$ as a consequence of Proposition 13. However the situation is different for non-abelian simple groups. At the end of this section we will show that for any positive integer t , it can be exhibited a non abelian simple group S such that S^t is CIG. It is not clear whether the number $\beta_G(S)$ can be arbitrarily large when G is minimal-exponent. One could be tempted to conjecture that $\beta_G(S) \leq 1$ if G is minimal-exponent and S is simple, but this is wrong. Here we construct an example with $\beta_G(S) = 2$.

Example. Let $T = \text{SL}(2, 41)$. We have that $Z = Z(T) = \langle z \rangle$ where z is the unique element of T of order 2, moreover T contains elements of order 8 and has exponent $8 \cdot 3 \cdot 5 \cdot 7 \cdot 41$. The factor group $S = T/Z = \text{PSL}(2, 41)$ has order $8 \cdot 3 \cdot 5 \cdot 7 \cdot 41$. The group T has a transitive permutation representation φ of degree 42 with $\ker \varphi = Z$; if $p \in \{3, 5, 7, 41\}$, then the wreath product $C_p \wr_\varphi T$ contains an element of order p^2 . Now consider

$$X = (V_3 \times V_5 \times V_7 \times V_{41}) \rtimes (T_1 \times T_2)$$

where

- $T_1 \cong T_2 \cong \text{SL}(2, 41)$, $V_p \cong C_p^{42}$,
- T_1 centralises V_5 and V_7 and acts on V_3 and V_{41} permuting the 42 entries,
- T_2 centralises V_3 and V_{41} and acts on V_5 and V_7 permuting the 42 entries.

Let $Y = \langle (z, z) \rangle \leq Z(T_1 \times T_2)$ and consider $G = X/Y$. Notice that $\exp(G) = 8 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 41^2$. Set $M = ((V_3 \times V_5 \times V_7 \times V_{41}) \times Z(T_1 \times T_2))/Y \leq G$ and notice that $G/M = S_1 \times S_2$ with $S_i \cong \text{PSL}(2, 41)$. Let now H be a subgroup of G with $\exp(H) = \exp(G)$. For $i = 1, 2$, consider the projections $\pi_i : HM/M \rightarrow S_i$

of HM/M onto the i -th factor of $G/M = S_1 \times S_2$. Since H contains elements of order 3^2 and 41^2 , $\pi_1(HM/M)$ must contain elements of order 3 and 41. However if U is a maximal subgroup of S , then $|U| \in \{41 \cdot 20, 60, 42, 40, 24\}$, and therefore we deduce that $\pi_1(HM/M) = S_1$. Furthermore, since H contains elements of order 5^2 and 7^2 , we have that $\pi_2(HM/M)$ must contain elements of order 5 and 7 and therefore $\pi_2(HM/M) = S_2$. Now suppose by contradiction that $HM/M \neq S_1 \times S_2$. This means that $HM/M = \{(s, s^\phi) \mid s \in S\}$ for some $\phi \in \text{Aut}(S)$. However H must contain an element h of order 8: it is not restrictive to assume that $h = (t_1, t_2)Z \in (T_1 \times T_2)Z$ with $t_2Z(T_1) = (t_1Z(T_2))^\phi$. In particular $|t_1| = |t_2| = 8$. But then $(t_1, t_2)^4 = (z, z) \in Y$ and $|h| = 4$, a contradiction. Thus, we have proved that if H is a subgroup of G with the same exponent, then $HM/M = S_1 \times S_2$.

Now let G^* be a subgroup of G minimal with respect to the property that $\exp(G^*) = \exp(G)$: then G^* is a minimal-exponent group and, by the above discussion, $\beta_{G^*}(S) = 2$.

We don't know other examples substantially different from the previous one; in particular we don't know whether it is possible to exhibit a minimal-exponent group G with $\beta_G(S) = 3$ for some non abelian simple group S . The situation is different if we consider finite PCIG groups. To construct our next examples, we need to introduce some more notations.

Let S be a non-abelian finite simple group. Define the set

$$\mathcal{X}_d = \{(x_1, \dots, x_d) \in S^d \mid \{x_1, \dots, x_d\} \text{ invariably generates } S\}$$

and consider the equivalence relation on \mathcal{X}_d : $(x_1, \dots, x_d) \sim (y_1, \dots, y_d)$ if and only if there exist $(s_1, \dots, s_d) \in S^d$ and $\alpha \in \text{Aut}(S)$ s.t. $(x_1^{s_1\alpha}, \dots, x_d^{s_d\alpha}) = (y_1, \dots, y_d)$.

For reader's convenience, we sketch the proof of the following elementary criterion.

Lemma 20. *Let $G = S^t$ for a non-abelian finite simple group S and an integer t . For $i \in \{1, \dots, d\}$, let $g_i = (g_{1,i}, \dots, g_{t,i}) \in S^t$. Then $\{g_1, \dots, g_d\}$ invariably generates G if and only if $(g_{i,1}, \dots, g_{i,d}) \in \mathcal{X}_d$ for all i and $(g_{i,1}, \dots, g_{i,d}) \not\sim (g_{j,1}, \dots, g_{j,d})$ whenever $i \neq j$.*

Proof. Consider the matrix R whose columns correspond to the elements g_1, \dots, g_d :

$$R = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,d} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,d} \\ \vdots & \vdots & \ddots & \vdots \\ g_{t,1} & g_{t,2} & \cdots & g_{t,d} \end{pmatrix}.$$

A necessary condition to have that $\{g_1, \dots, g_d\}$ invariably generates G , is that each row of R belongs to \mathcal{X}_d . This is not enough: we must be sure that no subgroup generated by conjugates of the elements g_1, \dots, g_d is contained in the diagonal subgroup $\{(h_1, \dots, h_t) \in S^t \mid h_i^\alpha = h_j\}$ for some choice of $i \neq j$ and $\alpha \in \text{Aut } S$. This is equivalent to say that no pair of different rows of the matrix R are equivalent. \square

As a first application of this Lemma, we show that $\text{Alt}(5)^t$ is CIG (and PCIG) if and only if $t \leq 2$.

Proposition 21. *The group $\text{Alt}(5)^3$ is not CIG, while the group $\text{Alt}(5)^2$ is PCIG.*

Proof. Let $S = \text{Alt}(5)$. The set of prime divisors of $|S|$ is $\{2, 3, 5\}$ and the representatives of its conjugacy classes are 1 , $\tau = (1, 2)(3, 4)$, $\rho = (1, 2, 3)$, $\sigma = (1, 2, 3, 4, 5)$ and σ^α where $\alpha = (1, 2) \in \text{Aut } S$. The elements $\tilde{g}_1 = (\sigma, \sigma)$, $\tilde{g}_2 = (\rho, \rho)$ and $\tilde{g}_3 = (\tau, 1)$ invariably generate $\text{Alt}(5)^2$, and hence $\text{Alt}(5)^2$ is PCIG and CIG. Now consider the case of $G = S^3$ and assume by contradiction that G admits a CIG-set X . Note that any invariable generating set of S has to contain an element of order 5 (otherwise suitable conjugates of the elements of this set are all contained in the same point stabilizer) and an element of order 3 (otherwise suitable conjugates of the elements of this set are all contained in the normalizer of a Sylow 5-subgroup). This implies that it is not restrictive to assume that the elements of X are the following: $g_1 = (\sigma^{\delta_1}, \sigma^{\delta_2}, \sigma^{\delta_3})$ with $\delta_i \in \{1, \alpha\}$, $g_2 = (\rho, \rho, \rho)$ and $g_3 = (\tau^{\epsilon_1}, \tau^{\epsilon_2}, \tau^{\epsilon_3})$ with $\epsilon_i \in \{0, 1\}$. Since $(\tau^{\epsilon_i})^\alpha = (\tau^{\epsilon_i})^{s_1}$ and $\rho^\alpha = \rho^{s_2}$ for some $s_1, s_2 \in S$, $(\sigma, \rho, \tau^{\epsilon_i})$ is equivalent to $(\sigma^\alpha, \rho, \tau^{\epsilon_i})$. Therefore, we have only two choices, up to equivalence, for the rows of the matrix R , whose columns are g_1, g_2, g_3 , namely (σ, ρ, τ) and $(\sigma, \rho, 1)$, but then by Lemma 20, $\{g_1, g_2, g_3\}$ cannot invariably generate $\text{Alt}(5)^3$, a contradiction. \square

We conclude by showing that for every $t \geq 1$ there is a PCIG group G with $\beta_S(G) \geq t$ for some choice of S .

Proposition 22. *For any positive integer t there exists a simple group S with the property that S^t is PCIG.*

Proof. If p is a large enough prime then $\text{Alt}(p)$ contains at least t 2-elements ρ_1, \dots, ρ_t which are not pairwise conjugate in $\text{Sym}(p)$. Let σ be a cycle of length p and let τ be a cycle of length 3. Consider the elements $g_1 = (\sigma, \dots, \sigma)$, $g_2 = (\tau, \dots, \tau)$, $g_3 = (\rho_1, \dots, \rho_t)$: then g_1, g_2, g_3 satisfy the criterium of Lemma 20, and hence $\{g_1, g_2, g_3\}$ is a PCIG-set for $\text{Alt}(p)^t$. \square

REFERENCES

1. M. Aschbacher, R. M. Guralnick, Some applications of the first cohomology group. J. Algebra, 90 (1984), 446–460.
2. A. Ballester-Bolínches, L. M. Ezquerro, Classes of finite groups, Mathematics and Its Applications (Springer), vol. 584, Springer, Dordrecht, 2006.
3. M. Bianchi, A. Gillio Berta, P. Hauck, Maximal supersoluble subgroups of symmetric groups. Ann. Mat. Pura Appl. (4) 159 (1991), 371–404.
4. H. Cardenas, E. Lluís, El normalizador del p -grupo de Sylow del grupo simétrico S_{p^n} , Bol. Soc. Mat. Mexicana, 9 (1964), pp. 1-6.
5. E. Crestani, A. Lucchini, d -Wise generation of prosolvable groups, J. Algebra 369 (2012), 59–69.
6. E. Detomi, A. Lucchini, Crowns and factorization of the probabilistic zeta function of a finite group, J. Algebra, 265 (2003), no. 2, 651–668.
7. E. Detomi, A. Lucchini, C. M. Roney-Dougal, Coprime invariable generation and minimal-exponent groups, preprint.
8. J. D. Dixon, Random sets which invariably generate the symmetric group, Discrete Math 105 (1992) 25-39.
9. J. D. Dixon, B. Mortimer, Permutation groups, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996.
10. W. Gaschütz, Praefrattinigruppen, Arch. Mat. 13 (1962) 418–426.
11. M. Giudici, Quasiprimitive groups with no fixed point free elements of prime order, J. London Math. Soc. (2) 67 (2003), no. 1, 73-84.
12. W. M. Kantor, A. Lubotzky, A. Shalev, Invariable generation and the Chebotarev invariant of a finite group, J. Algebra 348 (2011), 302–314.

13. M. Liebeck, C. E. Praeger, J. Saxl, Transitive subgroups of primitive permutation groups, *J. Algebra* 234 (2000), no. 2, 291361.
14. A. Lucchini, A. Maroti, On the clique number of the generating graph of a finite group, *Proc. Amer. Math. Soc.* 137 (2009), no. 10, 3207–3217.
15. J. Nagura. On the interval containing at least one prime number. *Proc. Japan Acad.* 28 (1952), 177-181.
16. U. Stammbach, Cohomological characterisations of finite solvable and nilpotent groups, *J. Pure Appl. Algebra* 11 (1977/78), no. 1–3, 293–301.

ELOISA DETOMI AND ANDREA LUCCHINI, UNIVERSITÀ DEGLI STUDI DI PADOVA, DIPARTIMENTO DI MATEMATICA, VIA TRIESTE 63, 35121 PADOVA, ITALY